39 Simulink 기반 자동차 부품 연계보안 기술 연구

소속 정보컴퓨터공학부 분과 D 팀명 AutoShield 참여학생 홍재왕, 레퐁푸, 석재영 지도교수 손준영

과제소개

과제 배경

자율주행, 커넥티드카 확산으로 ECU/센서가 CAN/Ethernet으로 긴밀히 통신하며 차량 전자화가 가속됨.

CAN 취약, Ethernet 노출로 해킹/스푸핑/리플레이 위험 증가 -> Simulink 모델링과 보안 검증 필요.

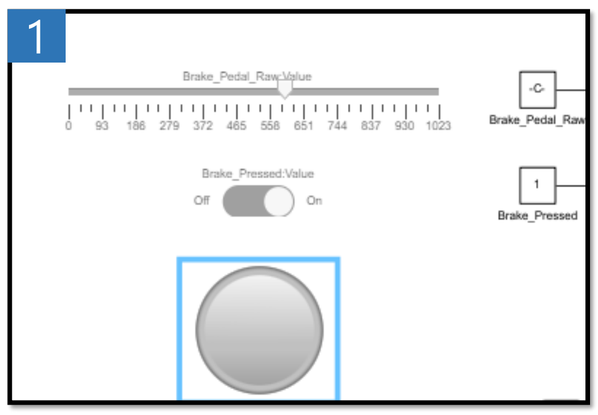
과제 목표

Vehicle Network Toolbox, MATLAB Function으로 통신, 보안 테스트 가능한 Simulink 환경을 구축하고, 메시지 흐름을 모델링.

CAN 취약점에 보안알고리즘을 통합해 유효 메시지 검증 체계를 구현, 평가.

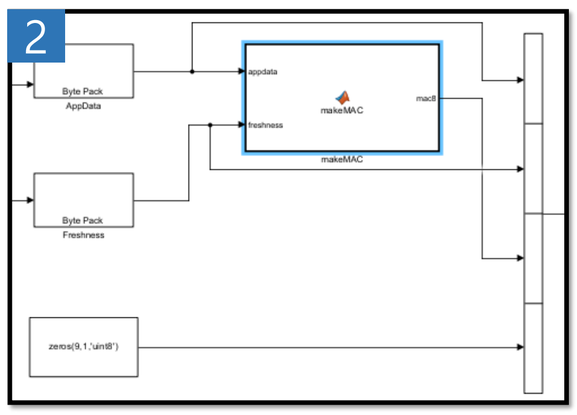
시스템 개요

1



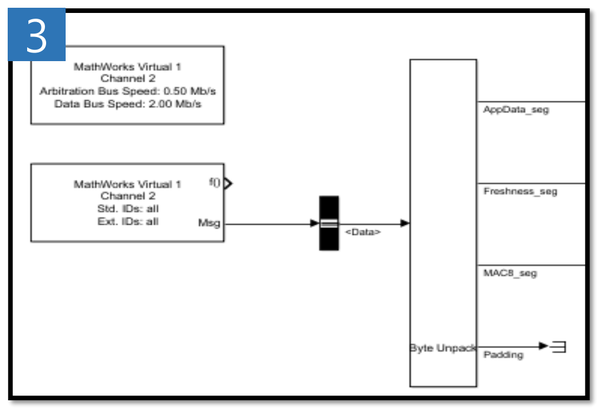
- Slider와 Switch를 활용하여 페달의 아날로그 값과 페달 눌림 여부 설정
- Lamp를 통해 데이터가 위변조 되지 않고, 유효성이 충족됐는지를 확인

2



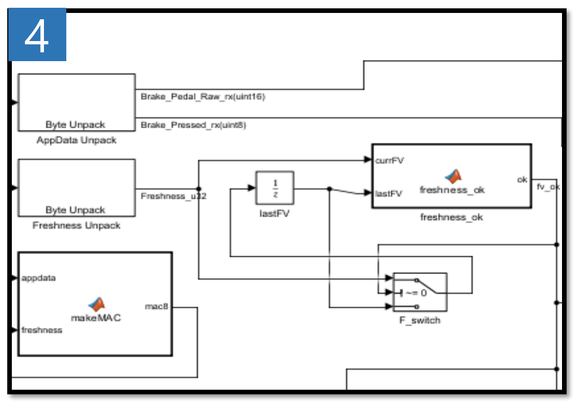
- Byte Pack과 makeMAC을 통해 입력된 데이터를 CAN 전송 형식으로 묶고, MAC을 붙여 보안성 강화

3



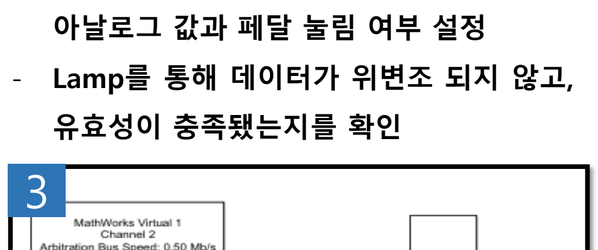
- 수신된 메시지를 다시 데이터/Freshness/MAC 값으로 분리

4



- makeMAC, Freshness_ok로 위변조 여부 확인 및 Freshness 유지 확인

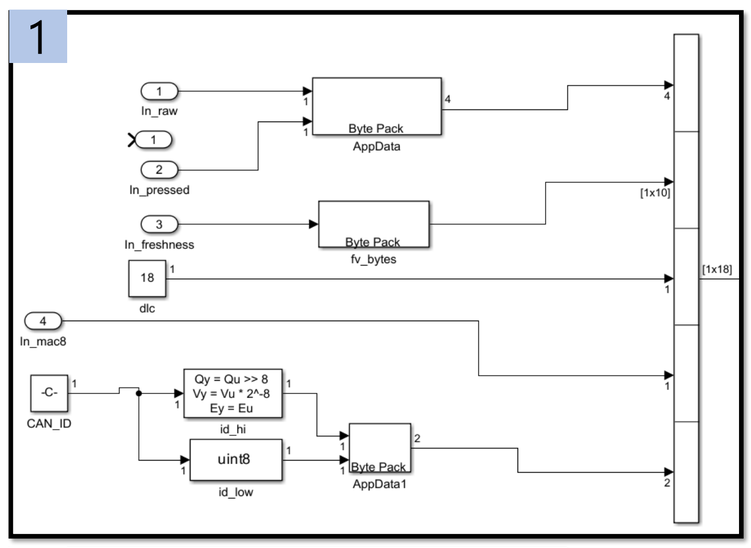
5



- 수신된 데이터가 올바른 값인지 확인

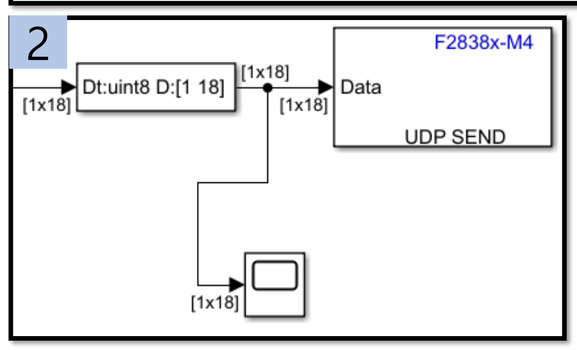
BrakeSensorECU_TX / ECU_RX

1



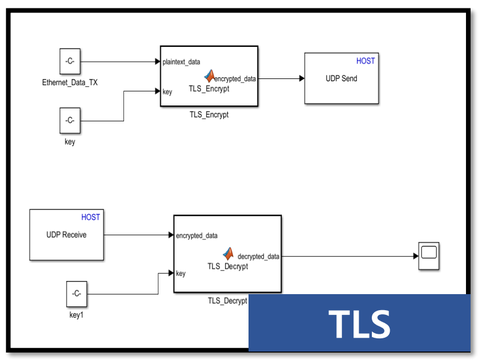
- BrakeSensorECU_TX에서 생성된 제동 관련 신호(Raw, Pressed, Freshness) 와 송신 측 MAC을 입력받아, Ethernet 전송용 PDU로 정규화/패킹한 뒤 UDP/TCP로 송신.

2

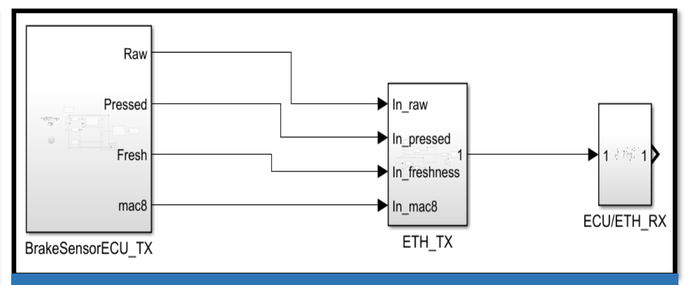


- CAN-FD 병렬 운용을 전제로 하며, 송/수신 동일 바이트 규칙(엔디안/필드 순서)을 보장.
- CAN-FD와 동일한 보안 규칙을 적용하여 수신부에서의 MAC/신선도 검증 일관성을 보장.
- Signal Specification으로 데이터 타입/차원을 강제함으로써 네트워크 블록 호환성 확보.

Ethernet_TX



TLS



Flow Chart

결론

결론

Simulink 기반 브레이브 ECU 보안 모듈 설계/구현

HMAC-SHA256으로 메시지 무결성 검증

CAN/Ethernet/TLS 적용 가능성 검토

기대 효과

CAN: 위변조/리플레이 공격 방어, 제동 ECU 신뢰성 강화

Ethernet: 고속/대용량 전송, 하이브리드 네트워크 적합성 확보

TLS: 암호화/인증 기반 통신으로 차량 네트워크 보안 강화